Responsible Business

At KeyBank, our values — teamwork, respect, accountability, integrity, and leadership — show up in how we work every day and guide the decisions we make. Strong governance and ethical business practices are the backbone of our company, and we hold ourselves and our third-party partners to high standards. We believe in continuous improvement and the importance of effective risk management. By investing in the right tools, technology, and processes, we stay prepared for evolving risks and regulatory changes to position us well for what's ahead.

Governance philosophy

Strong corporate governance from the top combined with effective risk management enables KeyBank to create shared benefit for all our stakeholders.

Board of Directors

The KeyCorp Board of Directors (the Board) is the top governing body of the organization. The Board oversees corporate governance, enterprise risk management, corporate strategies, and compliance. The Board also works with management through the Board committee structure to ensure clear decision-making and accountability for our actions — enabling alignment with shareholder expectations.

Our Board is committed to independent Board leadership, demonstrated through the guidance of our independent Lead Director, independent Board committee chairs, and full involvement of our independent directors (13 in total, excluding Chairman of the Board and Chief Executive Officer Christopher Gorman). Our Board believes that a robust and constructive Board and committee evaluation process is an essential component of Board effectiveness, and the Board conducts a yearly comprehensive evaluation process overseen by the Nominating and Corporate Governance Committee.

Standing committees of the Board

The Board delegates various responsibilities and authority to its five standing committees: Audit; Nominating and Corporate Governance; Compensation and Organization; Risk; and Technology.

Audit Committee

The Audit Committee oversees the integrity and transparency of the financial information provided to KeyCorp's shareholders. This includes reviewing financial disclosures in SEC filings, such as the annual Form 10-K, including any corporate responsibility and sustainability information that is incorporated within those filings.

Nominating and Corporate Governance Committee

The Nominating and Corporate Governance Committee oversees corporate governance matters generally, including KeyCorp's policies and practices on significant issues of corporate responsibility, including sustainability, community and governmental relations, charitable and political contributions, community investment strategy and activities, and fair and responsible treatment of consumer clients.

Risk Committee

The Risk Committee assists the Board with strategies, policies, procedures, and practices relating to the assessment and management of KeyCorp's enterprise-wide risks. The Committee also meets with senior leadership to review significant policies related to risk assessment, identification, management, and compliance. KeyCorp and its officers maintain responsibility for designing, implementing, and managing programs and policies for risk management.

Technology Committee

The Technology Committee assists the Board in fulfilling its oversight responsibilities with respect to the overall role of technology in executing Key's business strategy, including oversight of major technology investments supporting strategic objectives related to cybersecurity, fraud, data, innovation, and emerging trends; and in consultation with the Joint Risk Committee, provides oversight of technology-related risks.

Compensation and Organization Committee

The Compensation and Organization Committee is responsible for overseeing the compensation of Key's Board-reported Executives, compensation programs, and talent management and organizational development, including succession planning, leadership development, and strategic hiring objectives.

KeyCorp Board of Directors

Christopher M. Gorman
Chairman and Chief Executive Officer
KeyCorp

Todd J. Vasos
KeyCorp Lead Director, CEO
Dollar General Corporation

Jacqueline L. Allard
Group Head, Global Wealth Management
Scotiabank

Alexander M. Cutler
Chairman and CEO (Retired)
Eaton Corporation

H. James Dallas
SVP, Quality and Operations (Retired)
Medtronic, Inc.

Antonio DeSpirito
Managing Director (Retired)
BlackRock, Inc.

Elizabeth R. Gile
Managing Director (Retired)
Deutsche Bank AG

Robin N. Hayes
Chairman and CEO
Airbus of North America

Christopher L. Henson
Head of Banking and Insurance (Retired)
Truist

Richard J. Hipple
Executive Chairman (Retired)
Materion Corporation

Somesh Khanna
Co-Executive Chairman
Apexon, Inc.

Devina A. Rankin
EVP and CFO (Retired)
Waste Management, Inc.

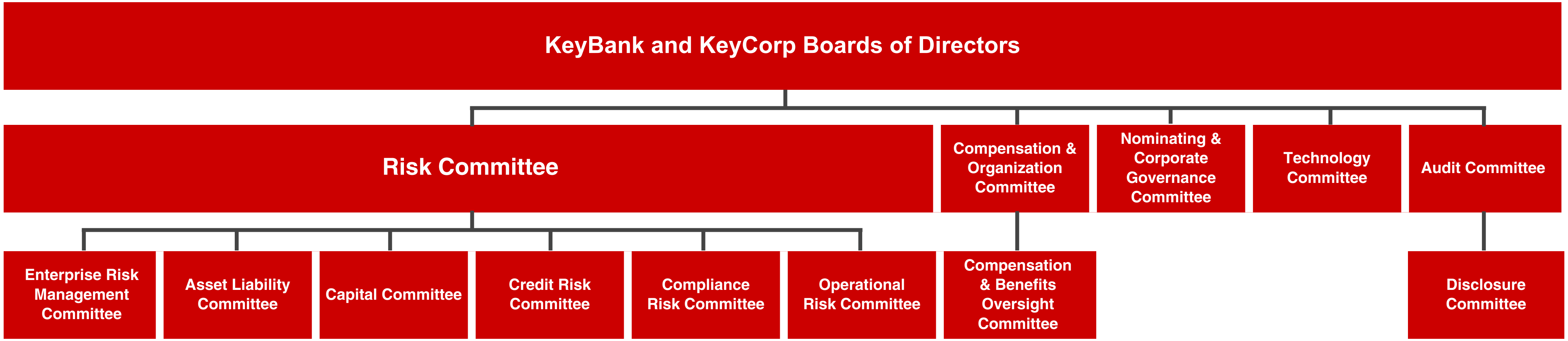
Barbara R. Snyder
President
Association of American Universities

Richard J. Tobin
President and CEO
Dover Corporation

David K. Wilson retired from the Board of Directors effective January 13, 2026. Ruth Ann Gillis and Carlton L. Highsmith retired from the Board of Directors effective at KeyCorp's 2026 Annual Meeting held on May 14, 2026. Additional information about KeyCorp's Board of Directors can be found in the latest Proxy Statement.

Risk Governance Committee Structure

The following table depicts our risk governance hierarchy.



Board oversight of risk

Our Board leadership and committee structure supports the Board's risk oversight responsibilities. Our Board and management committee structure enables the Board to exercise vigorous oversight of key issues relating to management development, succession and compensation, compliance and integrity, corporate governance and responsibility, cybersecurity, and company strategy and risk. With respect to risk, Board oversight ensures that KeyCorp's risks are managed in a manner that is effective and balanced and adds value for our shareholders.

The Board approves risk appetite, inquires about risk practices, reviews the enterprise portfolio of risks, assesses actual risks against the risk appetite, and is apprised of significant risks, both current and emerging — and determines whether management is responding appropriately. The Board challenges management and promotes accountability with respect to risk and other areas it oversees.

Enterprise Risk Management

Under the Risk Committee, Key has formed several senior-level management committees that report into the Risk Committee, including the Enterprise Risk Management Committee (ERM Committee). The ERM Committee is responsible for the implementation of Key's Enterprise Risk Management Policy (ERM Policy), encompassing our risk philosophy, policy framework, and governance structure for the management of risks across the entire company. The Risk Committee reviews the ERM Policy at least annually. The ERM Committee, along with other relevant senior-level management committees, ensures that our corporate risk profile is managed in a manner consistent with Key's risk appetite. The Board approves the ERM Policy and sets the overall level of risk Key is willing to accept and manage in pursuit of our strategic objectives.

Managing risk at Key

Effective risk management is conducted through understanding our business and the inherent risks within and outside the enterprise. Everyone at KeyBank is a risk manager, with a focus on risk identification and management to continuously integrate these activities into daily business processes.

Three lines of defense

To embed risk management into everyday processes while maintaining a strong foundation of oversight, the ERM Policy sets forth a “three lines of defense” model for risk governance that:

- Clarifies the general roles and responsibilities of the Lines of Business and Support Areas, Risk Management, and Internal Audit relative to the management of risk
- Provides a framework that supports the integrity of information escalated to our risk governance committees and to the Board and its committees

First Line of Defense

Lines of Business and Support Areas

The first line of defense is any organizational unit or function that is accountable for risk and either engages in activities designed to generate revenue; provides operational support or servicing to any organizational unit or function for the delivery of products or services to customers; or provides technology services to any organizational unit or function accountable for risk.

First line employees are responsible for owning and managing risk by overseeing the material business unit risk profile, operating within established limits, and integrating risk considerations into strategic decisions. This includes escalating material risks in a timely manner, ensuring compliance through appropriate procedures, and adhering to our risk management policies, practices, and controls.

Second Line of Defense

Risk Management

The second line of defense provides centralized oversight of enterprise risk by maintaining the ERM framework; delivering an integrated view of the risk profile; advising the business on acceptable risk levels; and ensuring material risks are effectively managed and escalated.

Second line of defense provides a credible challenge to risk-taking activities by the first line to ensure adherence with established Risk Policies and Programs and their related standards, procedures, and guidelines in alignment with the risk appetite established by the Board.

Third Line of Defense

Internal Audit

The third line of defense is Internal Audit, and it is responsible for independently evaluating the appropriateness of the risk governance framework for the size, complexity, and risk profile of Key. Internal Audit functions independently from our LOBs, support areas, and Risk Management and assists with coordinating external audit processes.

The three lines of defense are balanced in importance and stature, and they must all operate effectively across the enterprise to sustain strong risk management.

KeyBank maintains a moderate risk appetite

Risk appetite is defined as the level of risk we are willing to accept and manage in pursuit of our enterprise strategic objectives. Risk appetite is consistent with targeted risk-adjusted shareholder returns, the corporate risk-taking capacity, and balanced stakeholder interests. The risk appetite statement is an important component of our enterprise risk governance framework and reinforces the risk culture.

Our moderate risk appetite is articulated through qualitative statements, approved annually by the Board of Directors, and quantitatively reflected in metrics, limits, targets, and other measures at appropriate levels in the organization.

Major risk categories

We manage risk across eight major categories. These different risk types are often interrelated and affect various parts of the company.

Business conduct and ethics

At KeyBank, integrity is at the core of how we do business. We hold ourselves to the highest ethical standards across our enterprise, anchored to Our Code of Business Conduct and Ethics (the Code).

The Code plays a central role in advancing our purpose and reinforcing the workplace culture we commit to our employees. Our Ethics Office reviews and updates the Code each year, with input and oversight from the ERM Committee. It is then reviewed by the Audit Committee and approved by the Board.

Together, the Code and our values set clear expectations for how we conduct ourselves — guiding us to make sound decisions and uphold the highest professional and ethical standards.

Ethics and compliance training

All KeyBank teammates and directors are required to complete mandatory ethics training in a timely manner and are required to review and certify their understanding of the Code annually. To support ongoing awareness and understanding, we conduct roadshows that provide teammates with opportunities to learn about Code updates, ask questions, and receive guidance on applying ethical standards to real-world scenarios. These interactive sessions reinforce our commitment to transparency and help ensure all teammates have the resources they need to make informed, ethical decisions.

At the end of 2025, 98%[1] of employees and 100% of Board of Director members completed review and certification of their understanding of the Code. In addition, teammates are required to complete annual core compliance training and role-specific training.

Training topics include, but are not limited to:

- Fair and Responsible Banking
- Fraud Awareness and Escalation
- Protecting Key's Assets
- Managing Risk at Key
- Anti-Money Laundering
- Culture, Conduct, and Ethics

Report a concern

KeyBank employees and members of the KeyCorp Board of Directors are obligated to comply with the Code and to speak up when they suspect or witness a potential violation. Individuals can report concerns to a Code of Ethics Officer; contact the Ethics Office; call Key's Ethics Helpline; or complete an online form on our intranet, their personal computer, or smartphone.

Key's Ethics Helpline, administered by an independent third party, is available toll-free 24 hours a day, seven days a week. This helpline provides a safe and confidential way for teammates to report potential Code violations, with the option for callers to remain anonymous. We do not permit retaliation against individuals for reports of suspicious activity submitted in good faith, nor will disciplinary action be taken for such reports.

[1] Our goal is for 95% of employees to complete annual Code training; this allows us to accommodate new hires and employees who may be on extended leave.

Human rights

Key believes in and supports fundamental human rights for all people. We strive to create a workplace where people feel valued, affirmed, and empowered to do their best work as their authentic selves.

Read Key's Human Rights Statement.

Business conduct

KeyBank operates in a highly regulated environment and is obligated to comply with all applicable country, federal, state, and local laws, rules, and regulations. This includes all applicable securities laws, accounting standards, controls, and auditing practices.

Anti-bribery and anti-corruption

We remain steadfast in our adherence to all applicable anti-bribery and anti-corruption laws, such as the U.S. Bank Bribery Act, U.K. Bribery Act, and guidelines as provided by our Anti-Bribery & Corruption Policy. All Key employees, directors, service providers, and agents must act with transparency and integrity in all business dealings and follow all government requirements. Anti-bribery and anti-corruption training is included in the annual mandatory Code training.

Our Public Entities Policy strictly prohibits gifts and entertainment for public officials unless prior approval is obtained. Any offers or receipts of value from clients or third-party service providers that exceed the allowable limits of the Code must be disclosed to the Ethics Office promptly.

Anti-money laundering

KeyCorp fully supports the U.S. government's efforts to combat terrorism and money laundering. We maintain a comprehensive program of financial crimes governance policies, procedures, and guidelines designed to comply with all applicable U.S. Anti-Money Laundering (AML) and countering the financing of terrorism (CFT) laws. These policies apply to our domestic and international operations and are designed to identify and reasonably mitigate the risks resulting from illicit financial activity including terrorist financing, money laundering, and other related financial crimes.

Our Financial Crimes Governance policy is reviewed and approved annually by the Joint Risk Committee of the KeyCorp and KeyBank National Association Boards of Directors. As part of our AML program, we maintain reasonable procedures to verify the identity of each prospective customer and ascertain whether they are on the Office of Foreign Assets Control (OFAC) list or a similar list provided by a U.S. governmental or regulatory body when initiating a business relationship.

KeyBank maintains appropriate risk-based procedures for customers and enhanced due diligence, including the methods by which we develop an understanding of the nature and purpose of customer relationships, as well as the associated risks of potential financial crimes. We take our regulatory obligations seriously and are committed to meeting all applicable compliance requirements.

Read Key's Statement of Compliance with Anti-Money Laundering Laws.

Fair and responsible banking

At KeyBank, fair and responsible banking (FARB) is fundamental to our operations, demonstrating our commitment to treating each client with integrity and respect. FARB principles are embedded in all our business functions, policies, and practices and apply to all employees and third parties.

FARB laws, regulations, and regulatory guidance apply to all of Key's business functions, employees, and third parties acting on Key's behalf and are implemented throughout Key and its subsidiaries. The same principles of anti-discrimination and fairness apply to all employees, including customer relations, through Key's Code of Business Conduct and Ethics and the Professional Conduct Policy. Our FARB policies, programs, and practices are designed to identify, measure, monitor, control, and report FARB-related risks; provide a credible challenge to business activities across products and services; and support effective risk management activities related to fair lending and unfair, deceptive, abusive acts or practices (UDAAP).

FARB/CRA Risk Committee

Established in 2021, the FARB/CRA[2] Risk Committee oversees fair and responsible banking and Community Reinvestment Act risk activities. It ensures compliance with regulatory requirements and KeyCorp's Risk Appetite. The Committee monitors risks, trends, and issues across business segments and products, operating under the KeyCorp Enterprise Risk Management Policy.

Responsible sales and lending

FARB principles apply to all client interactions so that clients are fully informed about product risks and benefits. We make investments in products and services to support communities and clients at all stages of their financial journeys, including ways to save, pay down debt, buy a first home, and start businesses.

Managing complaints

Client feedback helps us improve our services. Our customer service professionals, including the Social Customer Care team, are trained to address complaints effectively. We use multiple channels to monitor feedback and have clear escalation processes for serious concerns. Complaints alleging discrimination are escalated to Enterprise Client Relations (ECR) for investigation. The FARB Complaint Management team conducts an additional review before ECR provides resolution.

Furthermore, we use complaint data to identify trends and areas for enhancement and to inform management of opportunities to improve the customer experience.

Employee training and reporting

To apply the FARB principles to client interactions effectively, KeyBank employees receive mandatory training based on their roles. Topics include, but are not limited to, Fair Lending and UDAAP, consumer advertising compliance, Key's Code of Business Conduct and Ethics, and managing risk. Employees are required to report any suspected regulatory violations to their managers or the Ethics Helpline. We maintain strict confidentiality for all reports to the extent possible, and Key strictly prohibits retaliation against any employee for making a good-faith report.

[2] The Community Reinvestment Act of 1977 (CRA) encourages certain insured depository institutions to help meet the credit needs of the communities in which they are chartered, including LMI neighborhoods, consistent with the safe and sound operation of such institutions. https://www.occ.gov/topics/consumers-and-communities/cra/index-cra.html.

Data privacy and security

Earning and maintaining trust starts with protecting the personal and financial information of all our stakeholders. With the adoption and accelerated use of artificial intelligence, it is more important than ever to continuously strengthen our security and privacy controls, manage emerging risks, and follow industry-leading standards to protect data and respond quickly and effectively to perceived or real threats and incidents.

KeyBank continues to advance our information security and privacy programs through strategic investments in technology. Our focus includes strengthening data security, maturing workforce identity and access management capabilities, modernizing customer identity verification, and advancing fraud detection. As digital engagement grows with our stakeholders, we are evolving client access and authentication to balance security with ease of use.

Governance oversight

KeyBank maintains a strong governance structure to oversee privacy, cybersecurity, and information security risks across the enterprise. Executive leadership and Board-level committees provide strategic direction and accountability to ensure these programs align with Key's broader risk management framework and regulatory obligations.

Privacy governance

Privacy governance is led by a dedicated Privacy team under the direction of the Chief Privacy Officer (CPO), who operates within the Compliance organization. The Privacy team reports to the Compliance Risk Committee, which in turn reports to the ERM Committee, and has authority to escalate material privacy risks to the Risk Committee of the Board. The Privacy team works in close collaboration with Cybersecurity and other Risk functions to implement controls and maintain compliance with applicable laws and regulations.

Key maintains a comprehensive internal Privacy Policy to protect personally identifiable information (PII), conduct lawful processing of information, and ensure compliance with applicable laws and regulations across the enterprise. The policy sets industry best practices as minimum requirements for processing PII, covering the entire data life cycle.

Transparency regarding our privacy practices is provided through Key's online privacy statement and consumer privacy notice, which describe how we collect, use, share, and safeguard PII, as well as the privacy rights available to individuals under applicable laws. Key does not sell PII and shares it only with contracted third parties for specific, necessary business purposes, or as otherwise required by law.

Information security governance

Information security oversight is led by the Chief Information Security Officer and the Chief Security Officer, who provide regular updates to Board-appointed committees on the status and effectiveness of Key's information security program. The Technology Committee of the Board oversees and approves the enterprise technology strategy, including cybersecurity capabilities, while the Risk Committee oversees the Information Security Policy and provides strategic guidance for its development and execution. Material risk management issues are escalated to the Risk Committee for review and action.

Additional details about our risk governance structure can be found in the Governance philosophy section.

Cybersecurity audits and assessments

We perform routine internal and external penetration testing to validate the strength and resilience of our security controls. Our cybersecurity posture is further reinforced through a robust third-party security program. On an annual basis, we assess our practices against recognized industry standards, including the National Institute of Standards and Technology Cybersecurity Framework and the Cyber Risk Institute Profile. Findings and insights from these evaluations are systematically incorporated to enhance and evolve our security strategy.

KeyBank is subject to cybersecurity and privacy regulatory exams as required by law for financial institutions operating in the U.S.

Our Internal Audit group performs independent internal audits to assess and enhance the effectiveness of our risk management, control, and governance processes. Any identified gaps are risk rated, assigned a due date for remediation, and tracked by Internal Audit to confirm that corrective actions are fully implemented and effective.

Incident management

Key's enterprise privacy and cybersecurity incident response plans establish clear governance, roles, and escalation paths for the Enterprise Cyber Response team to contain, investigate, and remediate incidents in a timely manner. They also support coordinated recovery of business operations following a cyberattack and provide structured processes for managing events involving bank information, including client and employee data.

Our Core Incident Response Rapid Emergency Assessment and Coordination Team (Core IR REACT) is responsible for responding to incidents, performing preliminary assessments, and engaging additional support team members as necessary. The Core IR REACT team can escalate issues to the Crisis Management Team (CMT), which includes the CEO and senior executives from Key’s lines of business and major support areas. The CMT provides overall strategic direction for incident response and recovery.

To safeguard client data, we employ robust security measures for online accounts, leveraging advanced data protection, strong encryption, and continuous monitoring to protect our clients’ accounts. Our online banking platform has strong sign-on requirements to safeguard sensitive information. We also regularly share security and fraud alerts with clients to help them protect their financial accounts. Our incident response protocols encompass both digital and physical security incidents, ensuring comprehensive protection of client and employee data regardless of the attack vector.

Our Privacy team assesses all incidents involving PII to ensure compliance with all applicable laws and regulations, including notifying affected individuals and regulators when necessary.

Privacy and security education

We execute robust cybersecurity, privacy, and fraud education and awareness programs for our employees, including annual mandatory training and ongoing campaigns on topics such as threat reporting, phishing, fraud scams, and security best practices. Physical security is a critical component of our holistic security approach, and our training programs include:

- Physical security awareness, such as identifying and reporting suspicious activity
- Workplace safety protocols, such as maintaining clean desk policies to protect sensitive information
- Secure document handling and disposal, particularly documents containing PII
- Visitor management, such as proper badge and access control usage
- Protection against social engineering tactics that exploit physical access

We provide clients and teammates with information and standard industry practices to keep individuals and businesses safe. In 2025, we created more than 100 educational assets focusing on physical security, cybersecurity, and privacy best practices. Content is promoted through client emails, account alerts, social media posts, newsletters, webinars, and information on our website. Additionally, we offer guidance on securing physical spaces, protecting personal devices, recognizing in-person fraud attempts, and safely conducting financial transactions at ATMs and branch locations.

Our approach to artificial intelligence

As artificial intelligence (AI) becomes more central to financial services, KeyBank is committed to using it responsibly, ethically, and transparently.

AI governance framework

Key's enterprise AI governance is overseen through our established risk governance framework. The Enterprise Risk Management Committee (ERM Committee) serves as the governing and approving body for Key's Artificial Intelligence Policy and provides enterprise-level oversight of AI risk in alignment with Key's risk appetite. AI risk management responsibilities are carried out across the three lines of defense to ensure appropriate ownership, independent review and challenge, and audit coverage. In practice, AI systems are required to be identified and inventoried; undergo governed intake and risk assessment; be deployed through approved channels; and be monitored and reported in alignment with Key's risk appetite. Board-level oversight of material AI risk exposures is provided through existing Board risk governance channels.

A shared AI lexicon was developed by the Artificial Intelligence Executive Oversight Group (AIEOG), a U.S. Treasury-led public-private partnership, to promote consistent terminology across the financial sector. Key has adopted the AIEOG AI Lexicon definition of AI (with minor adjustments for our context) to support consistent, risk-based oversight and governance across AI use cases.

AI risk management

Key's AI Risk Management Framework is aligned to the core functions of the National Institution of Standards and Technology AI Risk Management Framework (Govern, Map, Measure, and Manage) and is integrated with our broader enterprise policies, standards, and risk programs. This approach helps ensure AI risks are identified, assessed, managed, and monitored across the AI lifecycle, with governance and controls scaled appropriately based on risk.

Responsible AI principles

Key's AI use principles emphasize responsible design and risk-based governance, human-centered AI, accountability, transparency, understanding, security, privacy, safety, validity, reliability, resiliency, compliance with laws and regulations, and ethical use. We support these principles with risk-based testing and validation before release and monitoring after deployment, and we have selected an enterprise AI observability and evaluation platform to help standardize testing and ongoing monitoring for our generative AI / Large Language Model (LLM) solutions.

Responsible AI in action

Key has targeted several use cases of AI that are compliant with internal policies and our stated risk appetite. In 2025, we moved from pilots to delivering value in production. A major area of impact has been employee productivity: we expanded Microsoft Copilot; launched an internal retrieval-augmented generation platform that allows approved employees to ask questions grounded in approved corpora and receive sourced answers; and released enterprise agents via Copilot Studio to improve access to organization-wide knowledge.

Beyond knowledge management, AI has helped us improve efficiency in other areas. All use cases undergo comprehensive review through our AI governance process before deployment.

Transparency and accountability

Key's governance framework reinforces human accountability for AI-assisted outcomes and supports transparency and understanding appropriate to an AI system's intended use. We establish periodic reporting to relevant governance bodies, including the ERM Committee, on AI use, material AI risks, compliance, and significant findings.

Corporate Political Activity

Corporate political activity principles statement

At Key, we believe active participation in public policy advocacy is essential to informing better outcomes for the clients and communities that we serve and for the broader financial services industry. We engage in the political process to advocate for policies that promote economic growth, financial inclusion, and responsible banking practices — always within the bounds of applicable law.

While federal law restricts corporations and national banks from making direct political contributions to candidates, we maintain a robust framework for responsible political engagement. Our Government Relations department ensures all activities comply with federal, state, and local regulations. Our Law Group (referred to as Key Legal) and Compliance department provide rigorous oversight of our policies and procedures, while our Chief Ethics Officer enforces conflict-of-interest provisions detailed in our Code of Business Conduct and Ethics.

Board of Directors oversight

The Nominating and Corporate Governance Committee of KeyCorp's Board of Directors meets at least annually with a member of KeyBank's Government Relations team to review our policies and practices surrounding political contributions. This review includes our policies about doing business with public entities; the Government Relations pre-approval process for ballot issue support; substantive changes to regulations, if any, affecting Key's sponsored, separate, segregated funds; corporate political activity; and confirming that Key does not contribute corporate funds to candidate campaigns for election. This multi-layered governance approach ensures that our political engagement strategies are reviewed by our Government Relations team in coordination with Key Legal, the Compliance department, and the Chief Ethics Officer, creating a comprehensive system of checks and balances.

Lobbying expenditures

Our Government Relations program operates through a combination of in-house professionals and registered contract lobbyists who advocate on behalf of our business interests and the communities we serve. In 2025, our reportable federal lobbying expenditures totaled $1.1 million, which we invested in advocating for policies that support:

- Small business access to capital
- Community reinvestment and affordable housing
- Financial services modernization and innovation
- Consumer protection and financial education

We publicly disclose all lobbying activities in accordance with the Lobbying Disclosure Act and maintain strict compliance with federal, state, and local lobbying and reporting requirements. Our complete federal lobbying disclosures are available through the U.S. Senate's public database.

KeyCorp has earned Trendsetter status from the **CPA-Zicklin Index of Corporate Political Disclosure and Accountability** for six consecutive years — the highest recognition for corporate political transparency and accountability. This distinction reflects our commitment to rigorous oversight, comprehensive disclosure, and responsible political engagement.

Trade association membership and leadership

Key actively participates in industry trade associations at national, state, and local levels across multiple business lines. These relationships enable us to collaborate with peers on shared priorities such as financial system modernization, regulatory clarity, community development, and economic opportunity.

Our engagement spans the full spectrum of our business activities:

- **National banking and financial services:** We maintain active memberships in the Consumer Bankers Association (CBA) and Bank Policy Institute (BPI), where KeyCorp executives currently hold or have held a board member seat.
- **Housing and community development:** Through the National Association of Affordable Housing Lenders (NAAHL); the Mortgage Bankers Association (MBA), where a KeyCorp executive serves as a board member; and the Affordable Housing Tax Credit Coalition, we advance policies that expand access to homeownership and affordable housing.
- **Specialized financial services:** Our expertise in capital markets and leasing is represented through memberships in the Securities Industry and Financial Markets Association; the Securities Traders Association, where a KeyCorp executive serves as member chair; and the Equipment Leasing and Finance Association.
- **Inclusion in real estate:** We are proud members of the National Association of Hispanic Real Estate Professionals (NAHREP), supporting efforts to expand homeownership opportunities in underserved communities.
- **Regional leadership:** At the state level, we lead through active roles in bankers' associations and business organizations across our footprint. KeyCorp's Chairman and CEO serves as chair of the Ohio Business Roundtable (recently re-elected for a two-year term), helping shape business growth and economic development policy, while our regional executives advocate for sound, community-focused regulatory frameworks.

Key Impact |

Legislative impact: advancing affordable housing

Our advocacy efforts produce tangible results for the communities we serve. A prime example is our work on affordable housing policy at the federal and state level, where our collaborative engagement with policymakers and coalition partners helped advance legislation that expands housing access for low- and moderate-income families. Our work helps to:

- Increase funding for affordable housing development
- Streamline regulatory processes for housing construction
- Create new tax incentives for private investment in workforce housing
- Expand homeownership opportunities for first-time buyers

This legislative success demonstrates how our advocacy translates into real-world benefits — creating more affordable housing options, supporting economic mobility, and strengthening the communities where our clients and employees live and work.

Proactive engagement

KeyCorp takes a proactive approach to shaping public policy, focusing our advocacy on issues that directly impact our ability to serve clients and strengthen communities. Through consistent dialogue with elected officials, regulatory agencies, and community stakeholders, we advance policies in four key areas:

- Expanding financial inclusion and access to banking services
- Supporting small business growth through improved access to capital and streamlined lending processes
- Modernizing financial services regulation to foster innovation while maintaining robust consumer protections
- Enhancing financial education and consumer protection

Our government relations professionals and registered lobbyists maintain ongoing relationships with policymakers, providing data-driven insights on how proposed legislation would impact our clients, our communities, and our business.

Corporate political spending

It is important to note that KeyCorp does not contribute corporate funds for election campaigns. We prohibit supporting candidate committees, political parties or committees, or political action committees (PACs) organized for the advancement of political candidates. KeyCorp also does not contribute to Super PACs or independent expenditure committees, nor does the company make independent political expenditures in support of or opposition to candidates for public office.

As referenced previously in this section, Key may make contributions in support of certain ballot issues that in turn support the interests of our businesses, our employees, and/or our communities. Ballot issue requests are reviewed by Key Legal and then submitted for final approval to the executive leader of our Corporate Center. Contributions for approved ballot issues are reviewed annually by the Nominating and Corporate Governance Committee of the KeyCorp Board of Directors and are disclosed semiannually on the Corporate Governance page of key.com.

Political action committees

Eligible officers, managers, and professional employees of KeyCorp can participate voluntarily in the political process by making an individual contribution to the PAC sponsored by KeyCorp. Information about contributions by the KeyCorp Advocates Fund and the KeyCorp Advocates Fund – Federal is publicly disclosed and accessible at fec.gov. Information for the KeyCorp Advocates Fund – New York can be found at elections.ny.gov.

Voting time-off

We support our teammates' right to participate in the democratic process. To help all employees cast their votes, we provide Voting Time-Off for primary and general elections. Teammates are eligible for up to two to three hours of paid time off to vote, with specific allocations based on their state's legal requirements. This policy applies to all employees (except those on call or on commission only), with limited exceptions as required by state law. We proactively communicate this benefit before each election and encourage all eligible employees to exercise their right to vote.